Note

Four Pairwise Orthogonal Latin Squares of Order 24

ROBERT ROTH*

Department of Mathematics, California Institute of Technology, Pasadena, California 91125

AND

MATTHEW PETERS

Hale and Dorr, Counsellors at Law, 60 State Street, Boston, Massachusetts 02109

Communicated by the Managing Editors

Received March 3, 1986

We improve the lower bound for $N(24)$, the maximum size of a set of pairwise orthogonal Latin squares of order 24, from 3 (established in 1960 by Bose and Shrikhande (*Trans. Amer. Math. Soc.* **95** (1960), 191–209)) to 4. We obtain 7 sets of four squares from 7 sets of 3 pairwise orthogonal orthomorphisms of the group $\mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ which were found by a non-exhaustive computer search. © 1987 Academic Press, Inc.

We denote by $N(n)$ the maximum size of a set of pairwise orthogonal Latin squares of order n. (See [3] for a history of the study of $N(n)$ and [2] for a table of the best known lower bounds for $N(n)$.) Bose and Shrikhande [1] proved that if q is a power of a prime then $N(q^2-1) \geqslant N(q-1)$ so that in particular $N(24) \geqslant N(4) = 3$. We shall exhibit 7 sets of 4 pairwise orthogonal Latin squares of order 24 which arise from sets of orthogonal permutations of the abelian group $\mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

If G is a (not necessarily abelian) group, written additively, and σ and τ are permutations of G then σ and τ are said to be orthogonal if the function $x \mapsto x^\sigma - x^\tau$ is also a permutation of G. To each permutation σ of G one associates the Latin square L_σ (with rows and columns indexed by G) given by $L_\sigma(x, y) = x^\sigma + y$. The permutations σ and τ are orthogonal if and only if L_σ and L_τ are orthogonal. In searching for sets of pairwise

* Author's permanent address: Department of Mathematics and Computer Science, Emory University, Atlanta, Georgia 30322.

0097-3165/87 $3.00

orthogonal permutations of G it suffices to consider only those permutations which fix the identity, 0, of G and only those sets of permutations which contain the identity permutation, i, of G. Permutations orthogonal to i are called orthomorphisms and were introduced by Johnson, Dulmage, and Mendelsohn in [4], where they established that $N(12) \geqslant 5$ by exhibiting sets of 4 pairwise orthogonal orthomorphisms of the group $\mathbb{Z}_6 \oplus \mathbb{Z}_2$. (Orthomorphisms had been studied earlier by Paige and Hall in [6, 7, 8] under the guise of complete mappings: σ is an orthomorphism of G if and only if the function $x \mapsto -x^\sigma$ is a complete mapping of G. It was proved in these articles that the condition "the Sylow 2-subgroup of G is trivial or non-cyclic" is necessary for the existence of an orthomorphism of the finite group G and that this condition is sufficient when G is solvable.) Subsequently Schellenberg, van Rees, and Vanstone [10] established that $N(15) \geqslant 4$ by exhibiting 3 pairwise orthogonal orthomorphisms of $\mathbb{Z}_{15}$ each of which commutes with the permutation $x \mapsto -x$.

Henceforth G will denote the group $\mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and the element $(a, b, c) \in G$ will be denoted by the integer $4a + 2b + c$; so, e.g., 11 and 21 represent the elements $(2, 1, 1)$ and $(5, 0, 1)$, respectively. Each of the following 7 sets of 3 orthomorphisms of G, when taken together with the identity i, forms a set of 4 pairwise orthogonal permutations of G. The orthomorphisms comprising these sets, given in terms of their cycle decompositions, appear in Table I. Each of the sets is maximal with respect to pairwise orthogonality:

$$\{\sigma_1, \sigma_2, \sigma_3\} \quad \{\sigma_1, \sigma_2, \sigma_4\} \quad \{\sigma_1, \sigma_2, \sigma_5\} \quad \{\sigma_1, \sigma_2, \sigma_6\}$$
$$\{\sigma_1, \sigma_2, \sigma_7\} \quad \{\sigma_1, \sigma_8, \sigma_9\} \quad \{\sigma_1, \sigma_8, \sigma_{10}\}.$$

TABLE I

Orthomorphisms of $\mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$\sigma_1 = (0)(1, 2, 3)(4, 8, 16, 15, 20, 18)(5, 10, 23, 19, 14, 6, 11, 17)(7, 9, 22, 13)(12, 21)$

$\sigma_2 = (0)(1, 3, 2)(4, 12, 9, 7, 14, 16, 10, 5, 17, 21, 6, 19, 8, 22)(11, 20, 13, 18, 23, 15)$

$\sigma_3 = (0)(1, 5, 14, 3, 12, 19, 9, 8, 11, 23, 18, 13, 15, 7, 22, 16, 21, 4, 10, 20, 6, 2, 17)$

$\sigma_4 = (0)(1, 5, 12, 22, 11, 13, 10, 6, 3, 15, 9, 17, 7, 8, 2, 18, 16, 19, 4, 23, 14, 21, 20)$

$\sigma_5 = (0)(1, 6, 12, 5, 2, 16, 21, 10, 22, 20, 7, 15, 19, 11, 18, 9, 8, 4)(3, 14, 13)(17, 23)$

$\sigma_6 = (0)(1, 6, 14, 7, 10, 17, 15, 4, 22, 20, 21, 8, 11, 23, 9, 5, 2, 18, 3, 12, 16, 13, 19)$

$\sigma_7 = (0)(1, 6, 10, 9, 20, 21, 5, 23, 8, 7, 3, 13)(2, 19, 22, 16, 11, 18, 15, 17)(4, 14, 12)$

$\sigma_8 = (0)(1, 3, 2)(4, 12, 11, 23, 13, 19, 10, 6, 16, 8, 21, 7, 14, 17, 20, 15, 9)(5, 18, 22)$

$\sigma_9 = (0)(1, 4, 15, 7, 3, 12, 19)(2, 16, 13, 14)(5, 20, 22, 23, 10, 18, 9, 6, 8, 17, 21, 11)$

$\sigma_{10} = (0)(1, 4, 3, 15, 7, 12, 16, 22)(2, 19, 9, 23, 10, 8, 5, 6, 17, 13, 11, 18)(14, 20, 21)$

The orthomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_{10}$ seem to be unrelated to the orthomorphisms of $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ listed in [4] which established $N(12) \geq 5$.

Writing $\tau - \psi$ for the function $x \mapsto x^\tau - x^\psi$, we note that the permutations $\sigma_k - \sigma_j$, $i - \sigma_j$, and $\sigma_j - i$ arising from our 7 sets of orthomorphisms have varying cycle types and no patterns are easily discernible. (The same is true of the orthomorphisms in [4].) The 12 permutations arising from the set $\{\sigma_1, \sigma_2, \sigma_3\}$ appear in Table II.

Since σ_3, σ_4, and σ_6 have order 23, it is worthwhile to check whether any of these 3 permutations has the property that the non-identity elements of the group it generates are all orthomorphisms of G. (If this were the case then this group would consist of 23 pairwise orthogonal permutations of G which would yield a projective plane of order 24 having a homology of cycle type $1^{26}23^{25}$. Since $3^j \not\equiv -1 \pmod{23}$ for all j, the existence of such a homology is not ruled out by the theorem of Lander [5, Theorem 3.20, pp. 94–95].) Unfortunately, none of σ_3^2, σ_4^2, and σ_6^2 is an orthomorphism of G.

In closing we remark that our choice of σ_1 and σ_2 as the starting points of our computer search was extremely fortunate. There are far too many orthomorphisms of G (approximately 3.2×10^7 were generated in approximately 50 cpu hours on a VAX 8600 at Hale and Dorr and we estimate that there are at least 2.5×10^{13} in all) for a backtracking search for large pairwise orthogonal sets to run to completion. We previously (see [9]) ran the initial part of such a search on a VAX 11/750 at Emory University but found no such sets of size larger than 2: after approximately 50,000 cpu minutes fewer than 5 % of all possible extensions (to a pairwise orthogonal set of size at least 2) of the first orthomorphism on the list had

TABLE II

Permutations Arising from the Set $\{\sigma_1, \sigma_2, \sigma_3\}$

$\sigma_1 - i = (0)(1, 3, 2)(4)(5, 7, 6)(8)(9, 15, 11, 10, 13, 18, 14, 16, 23, 20, 22, 19, 21, 17, 12)$

$i - \sigma_1 = (0)(1, 3, 2)(4, 20, 6, 21, 9, 15, 19, 5, 23)(7, 22, 11, 18, 14, 8, 16)(10, 13)(12, 17)$

$\sigma_2 - i = (0)(1, 2, 3)(4, 8, 14, 6, 13, 7, 9, 22, 10, 23, 16, 18, 5, 12, 21, 11, 15, 20, 17)(19)$

$i - \sigma_2 = (0)(1, 2, 3)(4, 16, 10, 7, 17, 20, 9, 6, 13, 23, 8, 14, 22, 18, 21, 19, 11, 15)(5, 12)$

$\sigma_3 - i = (0)(1, 4, 6, 20, 10, 14, 13, 2, 19, 18, 23, 21, 9)(3, 15, 16, 5, 11, 12, 7, 17, 8)(22)$

$i - \sigma_3 = (0)(1, 20, 18, 7, 9)(2, 11, 12, 23, 5, 19, 10, 14, 13)(3, 15, 8)(4, 22, 6)(16, 21, 17)$

$\sigma_2 - \sigma_1 = (0)(1)(2)(3)(4)(5, 11)(6, 8)(7)(9)(10)(12)(13)(14)(15)(16, 21, 18, 19, 22, 17)(20, 23)$

$\sigma_1 - \sigma_2 = (0)(1)(2)(3)(4, 20, 7, 23)(5, 19, 6, 16)(8, 22, 9, 17)(10, 18, 11, 21)(12)(13)(14)(15)$

$\sigma_3 - \sigma_1 = (0)(1, 7, 15, 11, 6, 17, 20, 12, 22, 5, 4, 2, 18, 9, 14, 21, 16, 10, 3, 13, 8, 19, 23)$

$\sigma_1 - \sigma_3 = (0)(1, 23)(2, 10, 3, 13, 16, 18, 17, 4)(5, 20, 12, 6, 9, 14)(7, 15, 19)(8, 11, 22, 21)$

$\sigma_3 - \sigma_2 = (0)(1, 6, 9, 7, 8, 13, 21, 2, 16, 15, 20, 19)(3, 14, 11)(4, 22, 12, 10, 17)(5, 23)(18)$

$\sigma_2 - \sigma_3 = (0)(1, 22, 12, 18, 10, 9, 23, 21, 2, 8, 13, 5, 7, 16, 15, 4, 6, 17, 20, 11, 3, 14, 19)$

been examined. In fact, σ_1 is orthomorphism number 821 on the list and σ_2 is orthomorphism number 21 on the list of those which are orthogonal to σ_1. The heuristic reasons for selecting σ_1 and σ_2, although too lengthy to state here, can be obtained from the authors.

REFERENCES

1. R. C. BOSE AND S. S. SHRIKHANDE, On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler, *Trans. Amer. Math. Soc.* **95** (1960), 191–209.
2. A. E. BROUWER, "Lower Bounds for $N(v)$, the Number of Mutually Orthogonal Latin Squares of Order v." Lecture Notes, Mathematisch Centrum, Amsterdam, 1979.
3. M. HALL, JR., "Combinatorial Theory," 2nd ed., Ginn (Blaisdell), Boston, 1986.
4. D. M. JOHNSON, A. L. DULMAGE, AND N. S. MENDELSOHN, Orthomorphisms of groups and orthogonal Latin squares, I, *Canad. J. Math.* **13** (1961), 356–372.
5. E. S. LANDER, "Symmetric Designs: An Algebraic Approach," London Math. Soc. Lecture Note Ser. Vol. 74, Cambridge Univ. Press, London, 1983.
6. L. J. PAIGE, A note on finite abelian groups, *Bull. Amer. Math. Soc.* **53** (1947), 590–593.
7. L. J. PAIGE, Complete mappings of finite groups, *Pacific J. Math.* **1** (1951), 111–116.
8. L. J. PAIGE AND M. HALL, JR., Complete mappings of finite groups, *Pacific J. Math.* **5** (1955), 541–549.
9. C. M. PETERS, "Orthomorphisms of Groups and Pairwise Orthogonal Latin Squares," Master's thesis, Emory University, 1983.
10. P. J. SCHELLENBERG, G. H. J. VAN REES, AND S. A. VANSTONE, Four pairwise orthogonal Latin squares of order 15, *Ars Combin.* **6** (1978), 141–150.